REMARKS

[0001] Claims 1-30 are pending in this application. The Examiner has objected to the Specification, the Disclosure, and Claims 10-18, 20-28. Claim 29 stands rejected under § 101. Claims 3 and 5 are rejected under § 112 as indefinite. Claims 1-5, 9-14, 17-24, and 27-29 are rejected under § 102(e) as being anticipated by U.S. Patent 7,058,807 to Grawrock et al. (hereinafter "Grawrock"). Claims 6-8, 15-16, 25-26, and 30 are rejected under § 103(a) as being unpatentable over Grawrock in view of U.S. Patent Application 2004/0021968 to Zimmer et al. (hereinafter "Zimmer"). Applicants have amended Claims 1, 3-5, and 9-30. Applicants have also canceled Claims 2 and 8.

AMENDMENTS TO CLAIMS

[0002] Claims 10-18 and 20-28 have been amended to correct problems pointed out by the Examiner with dependencies in the Claims as submitted. Claim 16 is further amended to remove an unnecessary punctuation point.

[0003] Claim 1 is amended to clarify that the key management module seals a cryptographic key by cryptographically combining the cryptographic key with the measurement values in at least one PCR. The measurement values thus represent a trusted configuration of the trusted computing platform and can additionally be used to unseal the cryptographic key. Specification, ¶ 48. Claim 1 is further amended to incorporate substantially the limitation of Claim 2 with the additional limitation a cryptography module that uses the unsealed cryptographic key. Support for this amendment is found in Claim 2 and in the specification at paragraph 59.

[0004] Claim 4 is amended to make a clarification similar to that made for Claim 1 with respect to the key management module. Claim 4 is further amended to incorporate the limitations of canceled Claim 8, which provides the support for this portion of the amendment.

[0005] Claim 9 is amended to clarify that sealing the cryptographic key involves cryptographically combining the cryptographic key with measurement values representing a trusted configuration to a platform configuration. Support for the amendment is found in the specification at paragraph 48. The amendment further clarifies that unsealing the key involves using the measurement values to produce the cryptographic key. Specification, ¶ 49. Claim 19 is amended to incorporate substantially the same limitations as those described in connection with Claim 9, and support for the amendments are similarly found in the specification at paragraphs 48 and 49.

[0006] Claim 29 is amended to clarify that the apparatus comprises a logic unit. Support for this amendment is found in the specification at paragraph 20. Claim 29 as amended further specifies means for decrypting data on the data repository with the cryptographic key. Support for this amendment is found at least at Figure 4 (cryptology module 320) and the accompanying discussion.

[0007] Claim 30 is amended to specify that the key management module directs the ESS to seal a cryptographic key associated with a data repository by cryptographically combining the cryptographic key with a measurement value associated with the data repository, where the measurement value represents a trusted configuration of the trusted computing platform. Support for the amendment is found in paragraphs 48 and 49 of the specification.

RESPONSE TO OBJECTION TO SPECIFICATION

[0008] The Examiner has stated an objection to the specification for failing to provide antecedent basis for the term "computer readable storage medium" in Claims 9-18. In response, Applicants have amended paragraph 37 of the specification to clarify that instructions may be stored in computer readable storage medium. Applicants further note that the amendment does not introduce new matter into the specification as "computer readable storage medium" is used in originally filed Claims 9-18. MPEP §608.04(a).

[0009] The Examiner has also stated an objection to the disclosure since the list of inventors on the cover sheet of the specification is different than the list of inventors in the disclosure. Applicants respectfully note that Applicants have corrected the discrepancy through their July 30, 2004 Request Under Rule 48 Correcting Inventorship. The Request was received by the USPTO on the same date and is available through PAIR. The Request removed the name "Daryl Carvis Cromer" and added the name "David C. Challener". Included with the Request was a correct copy of the Oath and Declaration.

RESPONSE TO CLAIM REJECTIONS UNDER 35 U.S.C. § 101

[0010] The Office Action asserts that Claim 29 is directed towards non-statutory subject matter, and thus subject to rejection under §101. The Office Action asserts that Claim 29 lacks the necessary physical articles or objects to constitute a machine or manufacture within the meaning of 35 U.S.C. § 101. However, Claim 29 is directed to an

apparatus. Applicants assert that an *apparatus* by definition fits at least in the categories of a machine or manufacture.

[0011] Although Applicants disagree with the Examiner's position, to expedite prosecution, Claim 29 is amended to recite an "apparatus comprising a logic unit…." Support for this amendment is found in the specification in paragraphs 20 and 36-38. Applicants assert that a logic unit is clearly a physical item such that Claim 29 does not encompass functional descriptive material that is not tangibly embodied. As such, Claim 29 as amended overcomes the rejection under §101.

RESPONSE TO CLAIM REJECTIONS UNDER 35 U.S.C. § 112

[0012] The Office Action has rejected Claims 3 and 5 under § 112 for allegedly being indefinite; particularly, the Examiner points to the recitation of the "Trusted Computing Group computer system specification." Again, while the Applicants disagree with the Examiner's position, in order to expedite prosecution, Claims 3 and 5 have been amended such that they no longer recite the phrase: "Trusted Computing Group computer system specification." As such, the claims, as amended, overcome the Examiner's rejection under § 112.

RESPONSE TO CLAIM REJECTIONS UNDER 35 U.S.C. §102(b)

[0013] Claims 1-5, 9-14, 17-24, and 27-29 stand rejected by the Office Action as being anticipated by Grawrock. Applicants respectfully disagree. It is well settled that under 35 U.S.C. §102 "an invention is anticipated if… all the claim limitations [are] shown in a single prior art reference. Every element of the claimed invention **must be**

literally present, arranged as in the claim. The identical invention must be shown in as complete detail as is contained in the patent claim." *Richardson v. Suzuki Motor Co., Ltd.*, 9 USPQ 2d 1913, 1920 (Fed. Cir. 1989) (emphasis added). Appellants respectfully assert that every element of the amended Independent Claims is not present in Grawrock.

[0014] Claim 1 is amended to specify that the key management module seals a cryptographic key associated with a data repository by cryptographically combining the key with the measurement values in at least one PCR. It further specifies that the measurement values represent a trusted configuration of the trusted computing platform. The claim as amended further specifies that the ESS unseals the cryptographic key using the measurement values. In addition, Claim 1 specifies that the cryptography module encrypts data stored in the data repository and decrypts data read from the data repository using the unsealed cryptographic key.

[0015] As such, Claim 1 claims two separate levels, or stages, of encryption; first, the encryption key itself is encrypted by combining the key with measurement values representing a trusted configuration of the trusted computing platform. In addition, there is a second layer of encryption – once the key is decrypted, the data on the data repository remains encrypted. It should be noted that the key can not be decrypted if the same trusted configuration of the trusted computing platform does not exist for unsealing the key that was used to seal the key. The cryptography module then uses the decrypted key to encrypt data written to the data repository and decrypt data read from it.

[0016] In contrast, Grawrock only teaches a single layer of encryption; in particular, the encryption of, or seal, of a key. Grawrock seems to teach only that the private key is used to authenticate that a platform is an authorized member of a data

center. The private key is not used to protect the data on a data repository. Grawrock lacks a second level of encryption embodied in the recited cryptography module.

[0017] The Examiner cites to Col. 7, lines 1-19 of Grawrock as support for the assertion that Grawrock teaches a cryptography module. Applicants respectfully disagree. The cited portion refers to a "root encryption key" which is an extension or variation of the private key. The keys in Grawrock are not themselves keys to data of a repository; rather, they are used to authenticate a platform for inclusion within a data center. The keys in Grawrock are not used to "encrypt data stored in the data repository and to decrypt data read from the data repository" as stated in Claim 1.

[0018] In addition, Claim 1, as amended, specifies encrypting and unencrypting data in the data repository using an unsealed cryptographic key. As discussed above, Grawrock does not teach a second level of encryption, nor does Grawrock teach using an unsealed cryptographic key to encrypt and unencrypt other encrypted data. As such, Grawrock does not teach all of the limitations of Claim 1.

[0019] Grawrock does not teach using an unsealed cryptographic key to encrypt and decrypt data. In contrast, Grawrock teaches using cryptographic key pairs to authenticate platforms to part of a data center. As such, Grawrock does not teach the cryptography module of Claim 1. Similarly, Grawrock does not teach using an unsealed cryptographic key to perform further encryption and decryption operations on the data in a data repository. Claims 9, 19, 29 and 30 incorporate limitations similar to those outlined above. As such, Grawrock fails to teach the limitations of these claims for at least the same reasons given in connection with Claim 1. As such, Applicants respectfully assert that the claims as amended are allowable over Grawrock.

RESPONSE TO CLAIM REJECTIONS UNDER 35 U.S.C. §103(a)

[0020] Claim 6-8, 15, 16, 25, 26 and 30 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Grawrock in view of Zimmer. While Claim 8 has been canceled, its limitations have been incorporated into Claim 4. Applicants respectfully assert that the Claims as amended overcome the § 103(a) rejection.

[0021] The Examiner bears the initial burden of establishing a *prima facie* case of obviousness. *See* MPEP § 2142. In order to establish a *prima facie* case of obviousness, the prior art references combined must teach or suggest all of the claim limitations. MPEP § 2143. *Graham v. John Deere Co.*, 383 US 1, 148 USPQ 459 (1966) sets forth the factual inquiry necessary to determine obviousness. Briefly, the Examiner must: determine the scope and contents of the prior art; determine the differences between the prior art and the claims at issue; resolve the level of ordinary skill in the pertinent art; and consider objective evidence present in the application indicative of obviousness or nonobviousness.

[0022] Applicants respectfully assert that the Office Action fails to establish a *prima facie* case of obviousness. First, not all elements of the amended claims are taught or suggested in the art of record; second, the factual inquiry of *Graham* weighs in favor of non-obviousness; and third, the Examiner has failed to present a sufficient case for obviousness. Applicants hereby consider the elements set forth in *Graham* in turn.

Scope and Content of the Art

Grawrock

[0023] Grawrock provides a solution to the problem of servers IP snooping and masquerading as legitimately being associated with other servers which comprise a data center. Col. 1, 6-15. For example, a server may pretend to be associated with a web site and receive personal and financial information from a user. Col. 1, 15-20. To combat this problem, Grawrock teaches using the facilities of a server complying with the Trusted Computing Platform Alliance (TCPA) to validate servers/platforms which seek to be associated with a particular data center.

[0024] The method involves generating a cryptographic key pair and storing the private key within the platforms. Abstract. This private key may be sealed to the individual platforms. Col. 10, 41-45. A challenger unit may then use the public key of the key pair to challenge the platform and verify that it is part of the data center. Col. 13, 54-46. In this manner, the platforms representing themselves as part of the data center can be authenticated as being legitimate participants.

Zimmer

[0025] Zimmer teaches a method for providing a secure firmware update in a TCPA-type system. Abstract. In particular, Zimmer discusses a trusted update in a pre-boot operational environment. Zimmer, ¶ 11. As such, Zimmer provides a method and manner for ensuring that only a valid BIOS/firmware update occurs by providing secure storage for certificates such that they are not susceptible to attack or corruption. Zimmer, ¶ 4.

Differences Between the Prior Art and the Claims at Issue

[0026] The first major difference is that the prior art and the claims at issue are directed to different problems. Namely, Grawrock is directed at the problem of network security and server authentication. Zimmer is directed at providing a secure firmware update. In contrast, the present invention is directed to the problem of securing data on a data repository (such as a hard drive) and protecting the key used to decrypt the data from interception by snooper code. While all three reference make use of, a TCPA computing platform, that alone is not evidence of a common purpose.

[0027] Second, as discussed above, the claims make use of two separate levels of encryption by using a key to decrypt and encrypt the data on the data repository, and then having the key itself encrypted in such a way that a change in the computing platform accessing the data repository cannot decrypt the key if changes have occurred to the platform since the key was sealed. These two levels of encryption ensure that the key cannot simply be discovered via a hard drive swap, insertion of snooper code into the BIOS, or through use of a rogue operating system. Neither Grawrock nor Zimmer teach a key needed to access a data repository where the key itself is also sealed or cryptographically combined with the platform configuration.

[0028] Third, certain claims (such as Claim 4 that includes the subject matter of Claim 8) specify that the sealing and unsealing of the cryptographic key, and the provision of the key to the data repository, occur before the operating system loads. Grawrock, as noted by the Examiner, does not teach such a limitation. While the

Examiner asserts that Zimmer teaches this limitation at paragraph 17, Applicants respectfully disagree.

[0029] As noted by the Examiner, Zimmer discloses at paragraph 17 enabling TPM functionality for authentication purposes during and after pre-boot. Applicants note that this is not the same as reading a sealed key, unsealing the key, and then providing the key to the data repository before the operating system loads.

[0030] In particular, neither reference teaches providing the key to the data repository. As discussed above, Grawrock and Zimmer do not teach an encrypted data repository which requires a key for decryption of its data. Nor does either reference teach performing this operation before the operating system loads. In contrast to both references, the present claims encompass two levels of encryption. The key is provided to the data repository to allow for decryption of information on the repository, including boot code that is used to load the operating system and/or the operating system itself. By providing a key to the data repository before the operating system loads, embodiments of the present invention as claimed provide an additional layer of security and protection against rogue operating systems. The claimed cryptography module uses the unsealed key to decrypt the data repository and read the data, that data may or may not include boot code for loading an operating system.

[0031] Finally, certain claims (such as Claim 30) identify the use of a removable data repository which stores the sealed key associated with the data repository. Grawrock does not teach storing any of the key pairs on a removable data repository; to the contrary, it only discusses storing the key on the platform itself. Zimmer discusses

removable media, but does not indicate that the removable media is used to store a sealed key; rather, the removable media simply contains the firmware driver. Zimmer, ¶ 13.

Ordinary Skill in the Pertinent Art

[0032] Several considerations are necessary to determine the level of one having ordinary skill in the art. "Factors that may be considered in determining the level of ordinary skill in the art include (1) the educational level of the inventor; (2) type of problems encountered in the art; (3) prior art solutions to those problems; (4) rapidity with which innovations are made; (5) sophistication of the technology; and (6) education level of active workers in the field." *Environmental Designs, Ltd. v. Union Oil Co.*, 713 F.2d 693, 696, 218 USPQ 865, 868 (Fed. Cir. 1983), cert. denied, 464 U.S. 1043 (1984); see also, MPEP § 2141.03.

[0033] Here, the field of endeavor is software, and the education level of the inventors is typically a college degree. The relevant types of problems relate to protecting data on a data repository using encryption, and further protecting the encryption key from being discovered via snooping. Prior art solutions to the problem provide only protection of the data repository through an encryption key, no protection of the encryption key itself as in the claimed invention. The speed at which innovations are developed is typical of other software areas. The technology itself is of normal complexity and requires workers with an understanding of trusted computing platforms and cryptography generally.

Evidence Present in the Application Indicative of Obviousness or Non-Obviousness

[0034] The test for obviousness is what the combined teachings of the references would have suggested to one of ordinary skill in the art. In re Keler, 642 F.2d 413, 425, 208 USPQ 871, 881 (CCPA 1981). Applicants respectfully assert that the invention presented in the application is sufficiently distinct from the prior art taught in Grawrock and Zimmer to constitute a non-obvious improvement.

[0035] As discussed above, the claims as amended have two separate layers of encryption which provides protection to both the key itself and to the underlying data in the data repository that the key unlocks. By using two layers of security, the key cannot be 'sniffed' out by code such that the platform is tricked into giving the code to an unauthorized snooper. In certain embodiments, additional security is provided by storing this key on removable media. Neither Grawrock nor Zimmer discuss double encryption at two distinct points as claimed.

[0036] In addition, the two references address different problems from that of the present application. Grawrock deals with authentication, while Zimmer deals with firmware updates. In contrast, the Claims deal with encryption of a data repository and encryption key protection. One of skill in the art working on data repository encryption would not look to references dealing with authentication and firmware updates in looking for a solution. As such, given the different problems addressed by Grawrock and Zimmer, there is no motivation or suggestion to combine the teachings of the two references to reach the claims.

[0037] Neither Grawrock nor Zimmer teach two levels of encryption as specified in the claims. Nor does either reference teach reading the sealed key, unsealing the key, and providing the key to the data repository before the operating system loads. In addition, the references fail to teach using removable media to store the key. As such, the references do not teach all of the limitations of the claims either separately or in combination. Applicants respectfully assert that the claims, as amended, are not obvious in light of the Grawrock and Zimmer references.

CONCLUSION

[0038] As a result of the presented amendments and remarks, Applicants assert that Claims 1, 3-7, and 9-30 are patentable and in condition for prompt allowance. Should the Examiner require additional information, Applicants respectfully request that the Examiner notify them of any such need. If any impediments to the prompt allowance of the claims can be resolved by a telephone conversation, the Examiner is respectfully requested to contract the undersigned.

Respectfully submitted,

Date: September 26, 2007

_/David J. McKenzie/_____

Kunzler & McKenzie
8 E. Broadway, Suite 600
Salt Lake City, Utah 84101
Telephone: 801/994-4646

David J. McKenzie
Reg. No. 46,919
Attorney for Applicants